POLITICA DE CORREO ELECTRONICO E INTERNET

1. INDICE

2. OBJETIVO

Ofrecer a los usuarios una guía sobre los requerimientos mínimos que deben ser cumplidos respecto de la política de correo electrónico e internet que provee el Gobierno Regional Metropolitano de Santiago, para sus usuarios como también las implicancias de su mal uso.

Es importante mencionar que el uso inapropiado de los recursos dispuestos para los usuarios, expone a la institución a riesgos innecesarios como los virus informáticos, interrupción de las redes y sus sistemas, A través de la aplicación de esta Política evitar problemas jurídicos tanto nacionales como internacionales.

3. ALCANCE

La Política mencionada en el presente documento cubre el uso apropiado del correo electrónico que es enviado y recibido desde y hacia el correo electrónico del Gobierno Regional Metropolitano de Santiago y al uso apropiado de los servicios de internet y aplica a todos los empleados, proveedores, contratistas, personal que esté vinculado con las firmas que presten servicios al Gobierno Regional Metropolitano de Santiago o que estén relacionados. Se incluye, además, todas las dependencias que son parte de la institución y a quienes transiten por la red del Gobierno Regional Metropolitano de Santiago.

4. ROLES Y RESPONSABILIDADES

El Jefe del Departamento de Informática: será el encargado de aplicar los filtros al servicio de correo que sean necesarios para el cumplimiento de estas normas, así como otros para el resguardo de la comunicación que transita por la red del Gobierno Regional Metropolitano.

El Departamento de Informática: respaldará semanalmente las cuentas de correo sin aviso previo a los usuarios, entendiendo que la información contenida es exclusivamente parte del trabajo habitual.

La infracción a las obligaciones establecidas en el artículo anterior, podrá constituir una violación al principio de probidad administrativa, y será sancionada en conformidad a lo dispuesto en la Ley N° 18.834, sobre Estatuto Administrativo. Lo anterior es sin perjuicio de la responsabilidad civil o penal que corresponda por el mal uso de esta herramienta.

Los usuarios: Cada usuario será responsable del correcto uso del correo electrónico y la navegación por Internet y del uso que se haga de estos servicios.

5. CONTROL NORMATIVO SSI

La siguiente política tiene por finalidad dar cumplimiento a los siguientes controles de la norma NCh-ISO27001.Of2013

Código del Control	Identificación del Control	Requisito de control
A.12.02.01	Controles contra códigos maliciosos	Se deben implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto con los procedimientos adecuados para concientizar a los usuarios.
A.13.02.01	Políticas y procedimientos de transferencia de información	Las políticas, procedimientos y controles de transferencia formal deben estar diseñados para proteger la transferencia de la información mediante el uso de todos los tipos de medios de comunicación.
A.13.02.03	Mensajería electrónica	La información involucrada en la mensajería electrónica debe ser debidamente protegida

6. DEFINICIONES

6.1 Uso Aceptable del Correo Electrónico

I. El uso de la cuenta de correo electrónico, de las redes y de los sistemas informáticos, proporcionados por El Departamento de Informática, debe guarda relación con el ámbito de competencia del Gobierno Regional Metropolitano de Santiago y tener como finalidad el ejercicio de las funciones propias e inherentes para las cuales el usuario ha sido contratado o se ha convenido su prestación de servicios.

II. Se promueve el buen uso del correo electrónico, de las redes y de los sistemas informáticos, especialmente aquellas prácticas que protejan al sistema de eventuales daños ocasionados por archivos o programas maliciosos.

III. Los usuarios deberán identificar en el correo sus datos (nombre, apellido, unidad), para que el receptor del mensaje identifique con certeza la identidad del remitente y la unidad de su procedencia.

IV. Para efectos de su uso personal, el usuario deberá tener cuentas de correo electrónico distintas a la institucional, utilizando servicios al proporcionado por el Gobierno Regional Metropolitano de Santiago. El uso de este tipo de servicio se encuentra sujeto a la misma normativa descrita en este documento.

V. Toda casilla de correo electrónico está directamente vinculada al funcionario para el cual fue creado, siendo este el responsable implícito del contenido escrito o adjuntado a él.

VI. Los usuarios son los únicos responsables de todas las actividades realizadas en sus cuentas de correo electrónico, debiendo cumplir en todo momento la normativa vigente.

6.2 Transferencia de Información en los correos electrónicos

I. La información intercambiada por este medio deberá restringirse a propósitos institucionales y el Gobierno Regional Metropolitano de Santiago estará facultado para aplicar todas las medidas necesarias para garantizar la estabilidad del servicio y su uso correcto sujeto a la ley vigente.

II. Se considerarán elementos de filtros para el envío de correos con archivos adjuntos, como tamaño máximo autorizado para el envío.

III. número máximo de archivos adjuntos,

IV. elementos criptográficos para proteger la integridad.

V. aplicaciones antivirus y antimalware para la recepción de correos con archivos adjuntos

Todo lo anterior es considerado como "uso aceptable del correo electrónico". Lo que no se ha incluido dentro de este marco, se considera como "uso no aceptable del correo electrónico".

6.3 Uso no aceptable del Correo electrónico.

De acuerdo a lo expresado en "uso aceptable del correo electrónico", lo que se presenta a continuación son conductas que caen dentro del ámbito delo uso no aceptable del correo electrónico, siendo un listado "no absoluto".

7. Mensajería electrónica

1. Los usuarios deberán mantener bajo reserva la contraseña de acceso de su cuenta de correo electrónico, evitando almacenarla o compartirla para evitar ingresos no autorizados. De ser almacenada en el sistema informático en el que se accede, deberá ser almacenada de manera protegida.

2. Los usuarios tienen prohibido intentar acceder en forma no autorizada a la cuenta de correo electrónico de otro usuario y tratar de tomar su identidad, salvo su expresa autorización.

3. Los usuarios deberán respetar la naturaleza confidencial de los datos que puedan ser de su conocimiento ya sea como parte de su trabajo o por accidente.

4. Los usuarios deberán usar un lenguaje respetuoso en sus mensajes con usuarios internos o externos y estos mensajes de ninguna forma podrán ser de contenido difamatorio, insultante, injurioso, amenazador, ofensivo, obsceno, racista o sexista.

5. Realizar hostigamiento o acoso laboral, sexual, político, o de cualquier otro tipo.

6. Se prohíbe el envío de información con fines de proselitismo político, religioso, u otro de carácter similar.

7. Se prohíbe emitir opiniones personales en foros de discusión, listas temáticas u otras instancias de naturaleza polémica con la cuenta de correo electrónico institucional o de las redes del Gobierno Regional Metropolitano de Santiago.

8. El correo electrónico es vulnerable a modificaciones o accesos no autorizados, por lo que no garantiza el envío seguro y confidencial de la información que la ley establece como secreta o reservada, debiendo el usuario abstenerse de enviarla por dicho medio, salvo que exista causa justificada y se procuren medidas que protejan la seguridad y confidencialidad de la información.

9. Los usuarios deberán abstenerse de enviar/recibir por e-mail contenidos que no tengan relación con el trabajo y que sean de gran tamaño tales como videos, imágenes, archivos de audio (mp3), etc.
10. Está prohibido al usuario el uso de seudónimos u otros sistemas para ocultar su identidad. En todos los mensajes debe estar claramente identificado el origen del mensaje.

11. Está prohibido al usuario enviar mensajes a otro usuario o grupo que no los quieran recibir.

12. La apertura de archivos adjuntos o la ejecución de programas que se reciban vía correo electrónico, constituye acciones que pueden vulnerar la estabilidad, calidad o seguridad de las redes o del sistema informático.

13. Se prohíbe el envío de cualquier tipo de publicidad o aviso comercial, cadenas de correo electrónico, comercialización de productos (compra y venta), pirámides, phishing, donaciones, peticiones de firmas o cualquier asunto que se circunscriba al mal uso del correo electrónico, salvo que se realice con motivo del cumplimiento de las funciones que sean propias.

14. Se prohíbe todo lo que se considere como contenido de naturaleza ilegal (relacionados con hechos delictivos, pudiendo ser terrorismo, piratería, documentos electrónicos con infracción al derecho de autor, pornografía infantil, estafas y otros).

15. El usuario no deberá enviar por correo electrónico documentos que, individualmente o en conjunto, contengan más de 20 megabytes, salvo que el envío por otro medio o dispositivo electrónico, como CD, DVD, pendrive u otro, no sea posible. En todo caso, el usuario puede solicitar al Área de Soporte, la asesoría para determinar la mejor alternativa de compartir estos documentos.

16. Se prohíbe enviar SPAM o correo electrónico masivo no deseado por los destinatarios, salvo que ello fuese excepcional e indispensable para el mejor cumplimiento de sus funciones.

17. Se prohíbe utilizar los servidores de correo electrónico para retransmitir correos sin el permiso expreso de la autoridad correspondiente, debiendo cumplir la normativa vigente.

18. Se prohíbe la utilización de servidores de correos distintos a los utilizados por el Gobierno Regional Metropolitano de Santiago para el envío o recepción de documentos electrónicos propios de la institución. El Gobierno Regional Metropolitano de Santiago no dará soporte de servicios de correo electrónico que no sean los propios (ejemplo: gmail, yahoo, terra, etc.)

19. El uso de este listado de contactos difundidos por los sistemas de la institución, es solo para consultas y de uso exclusivo dentro del Gobierno Regional Metropolitano de Santiago. Está prohibido difundir cualquier listado (ej. Correos, teléfonos, y otro tipo de información pública) por cualquier medio electrónico o impreso para propósitos que no sean de uso institucional.

20. El Departamento de Informática no realizará respaldos de los correos ni de las carpetas locales de los usuarios, por lo que será de responsabilidad de éstos hacerlo. El usuario podrá solicitar al área

de Soporte, que se respalden dichos correos, utilizando algún procedimiento automatizado y asignar los recursos de almacenamiento según correspondan, previa autorización del jefe del solicitante.

7.1 Uso aceptable en la navegación de internet

- La navegación en internet, redes internas y el uso de los sistemas informáticos, proporcionados por el Departamento de Informática, debe guardar relación con el ámbito de competencia del Gobierno Regional Metropolitano de Santiago y tener como finalidad el ejercicio de las funciones propias e inherentes para las cuales el usuario ha sido contratado o se ha convenido su prestación de servicios. El uso del servicio de Internet implica aceptación integra de los términos, condiciones y avisos contenidos en el presente documento.

- Se promueve el buen uso de las redes y de los sistemas informáticos, especialmente aquellas prácticas que protejan al sistema de eventuales daños ocasionados por archivos o programas maliciosos.

- La información intercambiada a través de la Internet deberá restringirse a propósitos institucionales y el Gobierno Regional Metropolitano estará facultado para aplicar todas las medidas necesarias para garantizar la estabilidad del servicio y su correcto uso, sujeto a la ley vigente.

Los funcionarios son los responsables de aplicar un buen juicio para el uso razonable de los recursos.

7.2 Uso no aceptable en la navegación de internet

Todo lo anterior es considerado como "uso aceptable en la navegación de internet". Lo que no se ha incluido dentro de este marco, se considera como "uso no aceptable en la navegación de internet", siendo un listado "no absoluto".

El usuario debe abstenerse de:

- Causar algún daño grave e inminente en la calidad o estabilidad del servicio informático o de las redes.
- Transgredir los derechos de cualquier persona o compañía protegida por "Copyright", secreto comercial, patentes, regulaciones u otra propiedad intelectual, incluyendo, pero sin limitarse a la instalación o distribución de software, que no se encuentre apropiadamente licenciado para el uso de la institución.
- Exportar software, información técnica, tecnología, software de encriptación u otro que implique violación a la legislación internacional y nacional sobre control de exportaciones ilegales.
- Utilización de activos computacionales para actividades circunscritas como ilícitas.
- Introducir programas maliciosos a la red o servidores (ej. Troyanos, virus, malware, otros).
- Realizar ofertas fraudulentas de productos o servicios utilizando activos institucionales.
- Efectuar infracciones de seguridad, interrupciones de servicios, que incluyen, pero no limitan, al acceso de información, conexión a servidores, switch, firewalls sin una autorización expresa.
- En relación a interrupción de servicios incluye, pero no se limita a, inspección de tráfico, inundación por ping, falsificación de paquetes de red, denegación de servicios y falsificación de información de ruteo para fines maliciosos.
- Realizar cualquier tipo de escaneo o monitoreo de redes o seguridad a menos que exista una notificación de la unidad de seguridad o sea parte de la actividad de su trabajo.
- Eludir la autentificación de usuario o la seguridad de cualquier dispositivo, red o cuenta.

- Interferir o denegar cualquier servicio informático, utilizando programas, scripts, comandos o cualquier otro método, siendo realizados de forma interna o externa a la institución.

- Proveer información de cualquier tipo pertenecientes a la institución a partes externas, sin la debida formalización de la autorización.

- Se prohíbe todo lo que considere como contenido con naturaleza ilegal (relacionados con hechos delictivos, pudiendo ser terrorismo, piratería, documentos electrónicos con infracción al derecho de autor, pornografía infantil, estafas y otros).

8. Procedimiento de actualización antivirus

8.1 Control contra códigos maliciosos

EL Gobierno Regional Metropolitano implantará controles de detección como Programas Antivirus, Antimalware a nivel de usuario y muros cortafuegos y antivirus en los servidores de manera protegerse contra códigos malicioso, malware o virus informáticos a fin de mantener una red sana y estable para el servicio de los usuarios.

El Departamento de Informática cuenta con un sistema de protección antivirus a través de un software ESET EndPoint, Instalado en un Servidor Antivirus y diseñado para actuar en ambientes corporativos y que permite una completa protección a los equipos.

El servidor localizará todos los equipos disponibles en la Red e instalará individualmente a través de toda la red del Gobierno Regional Metropolitano mediante un paquete de instalación descargado desde el Servidor de antivirus en el cual se alojarán las respectivas versiones, sean de 32 o 64 bits.
Una vez copiado el paquete de instalación, éste se auto ejecutará y luego de un reinicio de la maquina quedará listo y protegida contra cualquier intrusión.
Las cuentas son en este caso serán los diferentes equipos a través de la red, siendo identificados por el servidor por el nombre de equipo y su respectiva dirección IP.

La actualización se hace de manera automática a través del mismo software que apuntará la última actualización existente en el servidor de antivirus, para finalmente actualizar la base da datos del antivirus. Esta herramienta, nos permitirá reconocer cualquier dispositivo que sea conectado al computador y poder escanearlo automáticamente evitando así intrusiones indeseadas.

Respecto del correo electrónico, este sistema de protección antivirus escaneara todos los archivos adjuntos, dejando pasar todo aquello que no represente un peligro o vulnerabilidad para los sistemas informáticos del Gobierno Regional Metropolitano, manteniendo lis sistemas libres de riesgos.
El sistema de antivirus tiene un protocolo de cifrado de información que funciona por un lado con la contraseña de usuario y la contraseña del buzón. La primera verifica la identidad del usuario y la segunda el contenido del correo.

Con todo lo anterior, los usuarios deberán:

- Para la navegación por internet, los usuarios deberán ingresar el usuario y contraseña del dominio institucional, mediante éste se le asignará un perfil de navegación internet.

- Mantener bajo reserva la clave de accesos, evitando almacenarla o compartirla para evitar ingresos no autorizados. De ser almacenada en el sistema informático en el que se accede, deberá ser almacenada de manera protegida.

- Respetar la naturaleza confidencial de los datos que puedan caer en su poder ya sea como parte de su trabajo o por accidente.

- Cerrar las sesiones activas en el computador cuando se finaliza la labor, a menos que se puedan asegurar mediante un sistema apropiado de control de acceso, como con protector de pantalla con una contraseña protegida, adicional al bloqueo estándar que aplica el Departamento de Informática.

- Por razones de seguridad y mantención de la red, solo los funcionarios del Departamento de Informática designados, podrán monitorear los equipos, sistemas y tráfico de la red, como medida de auditoria fundamental de la institución, según la periodicidad que sea necesaria para mantener un buen nivel de servicio.

9. DIFUSIÓN

El presente documento será difundido a través de correo electrónico a todo el personal del Servicio, así como también una copia de éste será publicada en la intranet Institucional.

10. PERIODICIDAD DE EVALUACIÓN Y REVISION

La siguiente Política será revisada, evaluada y/o actualizada según corresponda y aprobada su vigencia una vez al año por el Comité de Seguridad de la Información, en cuanto a su funcionamiento y correcta aplicación en la Institución.

11. FORMALIZACION EXTERNA

Mediante el acta fecha 23 de noviembre año 2021, se aprueba por parte del Comité de Seguridad de la Información, la Política de correo electrónico e internet.

12. REGISTRO DE REVISION Y ACTULIZACION HISTORICO

Versión	Autor	Paginas o secciones	Fecha Modificación	Motivo
01	Mauricio Marín	todas	12-02-2018	• Se fusiona con Norma de uso Navegación por Internet, Res Ex. N° 3043 del 22/12/17 y se agrega control 12.02.01
02	Mauricio Marín V.	todas	13/06/2018	Comité de Seguridad hace revisión de documento para el año 2018,
03	Mauricio Marín V.	todas	2/8/2018	Se cambia título 5 por Definiciones Se elimina título 10 respecto de Monitoreo Se cambia título 8 por Periodicidad y Revisión
04	Matias Benitez	Todas	08-07-2019	Se cambia pie de página
05	Matias Benitez.	Todas	12-07-2019	Comité SSI revisa y aprueba año 2019.
06	Carlos Hernández	12	16-11-2021	Se agrega capítulo 11 formalización externa Se actualiza índice
07	Carlos Hernández	Todas	23-11-2021	Comité SSI revisa y aprueba año 2021

13. FORMALIZACIÓN

Elaborado por	Revisado por	Aprobado por
Carlos Hernandez A. Analista Departamento de Informática	**José Gutiérrez G.** Encargado de Seguridad SSI **Paulo Mendoza R.** Encargado Unidad de Soporte **Carolina Hidalgo M.** Jefa Departamento Planificación y Control Institucional	**Mayuri Reyes T.** Presidente Comité de Seguridad

stgo GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO	**ACTA DE REUNION COMITÉ DE SEGURIDAD DE LA INFORMACION**	Página 1 de 3 Fecha 23/11/ 2021

ACTA DE REUNION: Comité de Seguridad de la Información	
Objetivo	Situación SSI año 2021
Fecha y Hora	23-11-2021, 15:00
Lugar	Sala de Reunión 2° Piso

PUNTOS DE LA REUNION

1. Bienvenida
2. Actualización de Documentos
3. Vulnerabilidades año 2021
4. 67 vulnerabilidades detectadas en sitios y páginas webs
    a. Caída de Switch piso 5 - 13 de septiembre 2021
    b. Caída de Switch piso 1 - 27 de septiembre 2021
5. Envío Correo Phishing
6. Protectores de Pantalla
7. Capacitación SSI
8. Mejoras
    a. Switch
    b. GTD Ancho Banda
9. SGD, 0 Papel
10. Eliminación Activos
11. Necesidades Tecnológicas

Aprobación los siguientes documentos

1. **Instructivo correctivo y preventivo contra fallas de energía y otras fallas de servicio**
2. **Manual de gestión de archivos**
3. **Norma de acceso a la Red**
4. **Norma de Eliminación de Activos**
5. **Norma de la Seguridad de la información para la Gestión de Proyectos**
6. **Norma de Outsourcing**
7. **Norma de Trabajo Remoto**
8. **Norma de uso identificación y autentificación**
9. **Norma de uso de instalación legal de software**
10. **Norma de reutilización y devolución de activos**
11. **Plan de Continuidad**
12. **Plan de emergencia Institucional**
13. **Política clasificación de activos**
14. **Política de acceso físico**
15. **Política de correo electrónico e Internet**
16. **Política de Derechos de propiedad Intelectual**
17. **Política de desarrollos de sistemas**

18. Política de dispositivos móviles
19. Política de escritorios y pantallas limpias
20. Política de gestión de incidentes de seguridad
21. Política de gestión de la capacidad
22. Política Gestión de Personas
23. Política de la seguridad informática
24. Política de respaldo de la información
25. Política general de seguridad de la información
26. Política gestión de claves
27. Política manejo de activos
28. Política sobre el uso de controles criptográficos
29. Procedimiento de control de las vulnerabilidades técnicas
30. Procedimiento de Controles de Auditoria de Sistemas de Información
31. Programa de concientización sobre seguridad de la información
32. Protocolo y control de tratamiento de SSI

DESARROLLO DE LA PRESENTACION

José Ignacio da la bienvenida y explica brevemente que es el SSI y las funciones del comité

Se da detalle al comité respecto a las vulnerabilidades CSIRT y las caídas de los switch

Claudio Muñoz y Mayuri Reyes, solicitan al comité la revisión de funcionamiento de cámaras de seguridad del Gore. Debido a problemas que existen actualmente

José Ignacio informa que esta demora se ha debido a que se necesita realizar una revisión inicial de todas las cámaras y su funcionamiento.

Se detallan las mejoras tecnológicas a realizar con carácter de importancia

- Cambios en los switch
- Importancia de dejar el sistema de cámaras en un circuito cerrado fuera de la red

Se recalca la importa de incluir SSI en la inducción a nuevos funcionarios

Se menciona a comité que se enviara cazabobos y que de ahí se realizara una capacitación a quienes caigan en él.

Se establece que el cambio de contraseñas debiera ser cada 6 meses de forma obligatoria empezando con un cambio masivo en marzo. Aplicándose tanto en AD como en sistemas.

Comité solicita que los mensajes de los protectores de pantalla sean un poco más "Rudos" refiriéndose a la gravedad de lo que podría ocasionar una vulneración importante de sistemas

Silvana Torres entrega información

- **Acerca del expurgo de documentos**
- **2022 se enviará soporte en papel a archivo nacional**
- **Se está digitalizando documentación antigua**
- **Menciona que para todo envío a archivo nacional o eliminación debe haber un testigo que vise la correcta digitalización de documentos, transformación digital 21808**

José Ignacio retoma la palabra e indica al comité la importancia dentro de todo el proceso de 0 papel de contar con una cloud de respaldo para toda la gran cantidad de archivos que se está generando

Explica que se continuara siempre con el respaldo en cintas. Indica que se necesita realizar respaldo en cintas como parte de SSI

Se aprueban políticas y documentación SSI

Carolina Hidalgo solicita curso de ciberseguridad a comité y participantes

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO	**ACTA DE ASISTENTES COMITÉ DE SEGURIDAD DE LA INFORMACION**	Página 1 de 1 Fecha 23/11/ 2021

N°	NOMBRE	DEPARTAMENTO O UNIDAD	FIRMA
01	José Ignacio Gutiérrez	Departamento de Informática	
02	Mayuri Reyes T.	División Administración y Finanzas	
03	Héctor Valladares	Departamento Jurídico	
04	Carolina Hidalgo	Departamento Planificación y Control Institucional	
05	Silvana Torres	Departamento de Gestión Documental y Activos	
06	Claudio Muñoz	Departamento de Servicios Generales	
07	Paulo Serrano	Departamento de Gestión de Personas	
08	Luz Magaly Nuñez	Unidad de Transparencia	
09	Ariel Lagos	Prevencionista de Riesgo	
10	VIRGINIA SAAVEDRA	DAF	
11			
12			
13			